IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
MIDLAND-ODESSA DIVISION

MALIKIE INNOVATIONS LTD., and KEY PATENT INNOVATIONS LTD. Plaintiffs, v. MARA HOLDINGS, INC. (F/K/A MARATHON DIGITAL HOLDINGS, INC.) Defendant.	CASE NO. 7:25-CV-00222-DC-DTG JURY TRIAL DEMANDED

PLAINTIFFS' SUR-REPLY CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

I. INTRODUCTION

Plaintiffs' constructions and arguments stay true to the intrinsic record and adhere to the governing legal principles and should be adopted. Defendant's constructions, which are not supported by the intrinsic record, impose unnecessary additional limitations (based mostly on extrinsic evidence), and run afoul of governing law, should be rejected.

II. ARGUMENT

A. The '286 Patent

1. "Montgomery-style reduction" *('286 patent - claims 1, 5, 6, 9)*

Defendant's Construction	Plaintiffs' Construction
"reduction that proceeds by clearing the least significant portions of an unreduced operand and leaving the remainder in the more significant portions"	This term appears only in the preamble and is not limiting.

The preamble is not limiting under the relevant legal framework, and Defendant fails to show otherwise. *See Arctic Cat Inc. v. GEP Power Prods., Inc.*, 919 F.3d 1320, 1327-29 (Fed. Cir. 2019). "Montgomery-style reduction" undisputedly does ***not*** supply antecedent basis for any term in the body of the claim and was ***not*** relied on during prosecution to distinguish the claims from prior art. *Id*. at 1329; *Am. Med. Sys., Inc. v. Biolitec, Inc.*, 618 F.3d 1354, 1359-60 (Fed. Cir. 2010). Defendant fails to identify any way in which the body of the claim is not "structurally complete," *i.e.*, Defendant identifies no necessary aspects of the claimed invention missing from the body and found only in the preamble. *Arctic Cat*, 919 F.3d at 1329; *Am. Med. Sys.*, 618 F.3d at 1360. Accordingly, under Federal Circuit precedent, the preamble term at issue is not limiting.

Defendant's Reply skips all the relevant inquiries and instead doubles down on inaccurate and irrelevant assertions about whether the claims as construed would read on purported prior art. Dkt. 59 at 1-2. The Federal Circuit has rejected this approach to claim construction. *Landers v. Sideways, LLC*, 142 F. App'x 462, 468 (Fed. Cir. 2005) (citing *Nazomi Commc'ns, Inc. v. ARM*

Holdings, PLC, 403 F.3d 1364, 1367-69 (Fed. Cir. 2005)). Despite Defendant's false claim to the contrary, Plaintiffs have never asserted or suggested that, without a non-limiting preamble, the claims would read on prior art; nor do Plaintiffs acquiesce to Defendant's improper and untimely invalidity arguments, which are issues to be dealt with *after* claim construction and are not properly before the Court during claim construction. *Id*.

Defendant's other arguments fall similarly flat. Defendant's citation to *UNILOC 2017 LLC v. Verizon Commc'ns, Inc.*, 2020 WL 805271, at *11 (E.D. Tex. Feb. 18, 2020) is inapposite. The preamble in *UNILOC 2017* provided "essential context" because it provided the antecedent basis for and further characterized a term in the body of the claim. *Id*. The term here does not. Neither does it describe "***how*** the method must proceed," as Defendant argues. Dkt. 59 at 2. Rather, the ***body*** of the claim recites how the method must proceed, by describing how each of the "obtaining," "computing," and "outputting" steps are performed. Dkt. 53 at 4-5. The preamble merely "employs the standard pattern" of a non-limiting preamble that "stat[es] a purpose or intended use." *TomTom, Inc. v. Adolph*, 790 F.3d 1315, 1323-24 (Fed. Cir. 2015).

Lastly, Defendant's "operand" versus "quantity" argument confirms that its construction reads out embodiments of the invention. Defendant contends the claim language itself requires the "operand" in the body of the claim to be an "unreduced quantity." Dkt. 59 at 3. Not so. The word "unreduced" appears nowhere in the claims, and nothing in the claims requires the claimed operand to be unreduced. The specification does not require it either and in fact teaches that the invention can be performed on a partially reduced operand (*e.g.*, at intermediate steps of a multi-step reduction). Dkt. 53 at 7-8. A partially reduced operand may be an "unreduced quantity" in the context of a given step or iteration where the invention can be performed, but the operand itself need not be unreduced. *Id*. Defendant's attempt to limit "operand" in the body of the claim to

"unreduced operand" through its improper construction of the preamble should be rejected.

2. "perform a replacement of a least significant word of the operand"
('286 patent - claims 1, 5, 6, 9)

Defendant's Construction	Plaintiffs' Construction
"add a modular equivalent of the operand's least significant word to the more significant words of the operand such that the result can be shifted down to drop the least significant word"	"replace a word that makes the smallest contribution to the value of the operand"

Defendant takes no issue with Plaintiffs' construction of "least significant word of the operand," so the Court should adopt that portion of the term. The remainder of the term—"*perform a replacement* …"—has its ordinary meaning, *i.e.*, replace. Dkt. 53 at 8-9. Nothing in the intrinsic record indicates otherwise. *Id.*; *see* '286 Pat., 3:31-39 ("the modified reduction value, when applied to the operand … performs a replacement for values in a low-order segment"); 5:59-60 ("[T]he value a_0 can be replaced with $a_0 \times n' \times 2^w$…."). Here, "perform a replacement" means what it says—replace. The claim elsewhere describes *how* that replacement is performed: by "using a reduction value." Where the patentee wanted to require specific types of reduction values used in performing the replacement, he added limitations specifying that, like in dependent claim 2. '286 Pat., 9:34-38 ("wherein the reduction value is $n'=2^{-w} \bmod n$, or a shifted or signed version of n'"). Accordingly, "replacement" in claim 1, as in the specification, has its ordinary meaning.

Defendant's construction improperly limits the claim to the use of a specific type of reduction value described in one embodiment of the specification. Dkt. 53 at 9-10. Defendant argues that "in order to correctly calculate the remainder" (even though the term "remainder" is not in the claims), "'replacement' in the context of the '286 patent must involve adding a modular equivalent of the LSW." Dkt. 59 at 4. But the "context" Defendant relies on is the patent's description of an embodiment that employes a *specific type* of reduction value, one not recited

(and therefore not limited to) in the claim. Dkt. 52 at 12-13 (citing '286 Pat., 5:59-67); Dkt. 59 at 5 (same). Defendant's expert admitted that the modular equivalence required by Defendant's construction comes from the way the reduction value in that particular embodiment is computed, *i.e.*, $n' = 2^{-w} \bmod n$.[1] Dkt. 53-5 at 56:5-57:12 ("**Q.** So the modular equivalence comes from the way n prime is computed? **A.** Yes. … **Q.** Okay. So that's what you're referring to, the computation of n prime where it equals 2 to the minus w mod n? **A.** Yes."). Each of the "examples" that Defendant created to support its unduly narrow construction employs that specific type of reduction value. Dkt. 52 at 8; Dkt. 52-2 at 23; Dkt. 59-2 at 5, 7, 9-10, 13.[2] But that type of reduction value is not required by claim 1, meaning claim 1 is not limited to that particular reduction value. Dependent claim 2, in contrast, recites this specific value, which underscores the broader scope of claim 1. *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 910 (Fed. Cir. 2004) ("[W]here the limitation that is sought to be 'read into' an independent claim already appears in a dependent claim, the doctrine of claim differentiation is at its strongest.").

Defendant's suggestion that Plaintiffs' construction of "perform a replacement" is somehow "inconsistent" and "cannot be reconciled" with their construction of "perform a cancellation" is nonsense. Dkt. 59 at 6. These are separate terms that refer to different actions: "perform a replacement" requires doing something while "rather than perform a cancellation" requires not doing another. '286 Pat., 9:27-32. Regardless, Plaintiffs' constructions are not inconsistent. That "cancellation" in this context refers to how the LSW is eliminated in a standard Montgomery reduction (which involves adding a multiple of the modulus to the operand), Dkt. 53

[1] The patent denotes the reduction value as n' (spoken "n prime").

[2] Defendant's "example" in Exhibit C to its Reply brief also employs this specific type of reduction value but multiplies it by a "randomly selected number" to demonstrate that doing so produces an incorrect result. Dkt. 59 at 4-5. That multiplying a random number by this specific type of reduction value produces an incorrect result is both unsurprising and irrelevant.

at 10-11, does not require "replacement" to mean anything beyond its ordinary meaning, *id.* at 8-10. Indeed, claim 1 expressly describes how the replacement is performed: "using a reduction value." Nothing more is necessary to understand the claim.

3. "perform a cancellation thereof" *('286 patent - claims 1, 5, 6, 9)*

Defendant's Construction	Plaintiffs' Construction
"add a multiple of the modulus to the operand such that the least significant word of the result is zero and the result can be shifted down to drop the least significant word"	"add a multiple of the modulus to the operand to eliminate the least significant word of the operand"

The parties agree that "perform[ing] a cancellation thereof" requires adding a multiple of the modulus of the operand. Dkt. 53 at 10. The parties disagree as to what the claim requires as a result of cancelling. Under Plaintiff's construction, cancelling "eliminate[s]" (*i.e.,* the ordinary meaning of cancel) "the [LSW] of the operand." That is consistent with the patent's description of a "typical implementation" of Montgomery reduction. '286 patent, 4:40-47; Dkt. 53 at 10-11.

Defendant's construction, on the other hand, introduces unnecessary terminology ("the least significant word of the ***result***") and leaves optional something that even the embodiment it cites notes is mandatory ("the result ***can be*** shifted down to drop the least significant word"), as discussed in Plaintiffs' responsive brief. Dkt. 53 at 11. Defendant's construction also requires "zeroing" and "shifting" to be the techniques required in cancelling, but that is only one embodiment – what the specification calls a "typical implementation." '286 patent, 4:40-47; Fig. 4. But all that is required under the plain meaning of "cancelling" is "eliminating" the LSW – nothing compels doing it in accordance with the example discussed in the specification.

Defendant offers that it "does not object" to a construction that "require[s] shifting or truncating to drop the zeroed LSW," but that does not cure the issue of limiting "cancelling" to a particular embodiment. But in order to come closer to Defendant's word choice, Plaintiffs would

agree to a construction of "add a multiple of the modulus to the operand to ***drop*** the least significant word of the operand."

B. The '062 and '960 Patents

1. "finite field operation"

('960 patent - claims 3, 6; '062 patent - claims 1-4, 6, 7)

Defendant's Construction	Plaintiffs' Construction
"operation where each operand is a finite field element"	"operation in a finite field"

"Finite field operation" should be construed to have its plain and ordinary meaning, which is, "operation in a finite field." Dkt. 53 at 13; Dkt. 53-2 ¶¶ 83-85; '960 Pat., 4:10-12 ("In general terms, the invention provides … methods for operating on elements in a finite field."). Plaintiffs' construction tracks that meaning.

Defendant's construction is both redundant and unduly limiting. It is redundant because it repeats that the finite field operation has finite field element operands—*i.e.*, that the operation is performed on finite field elements—which is already clear from the claims themselves. *See, e.g.,* claim 3 of the '960 Patent and claim 1 of the '062 Patent ("A method of performing a finite field operation ***on elements of a finite field*** …" ('960 Pat., 17:30-31; '062 Pat., 16:27-28))[3]; *see also* claim 3 of the '960 Patent ("***representing each element*** as a predetermined number of machine words" and "***performing*** a non-reducing wordsized operation ***on said representations***, said wordsized operation corresponding to said finite field operation" ('960 Pat., 17:32-36)); claim 1 of the '062 Patent ("obtaining a first set of instructions for performing the finite field operation ***on values representing the elements of the finite field***" ('062 Pat., 16:29-31)).

Defendant's construction is unduly limiting because its inclusion of the "each operand"

[3] Defendant agrees that this term should be construed in a manner consistent with its use in the claims' preambles. Dkt. 52 at 16.

requirement narrows the claim to the point of excluding preferred embodiments. The term "operand" is not in the intrinsic record. And limiting "finite field operations" only to those operations where "each operand" is "a finite field element" excludes operations on elliptic curve points, which are not single finite field elements but rather a *pair* of them. Dkt. 59 at 7-8. Nothing in the intrinsic record supports such a restriction, Dkt. 53 at 13-14; instead, the specification teaches the opposite, *i.e.*, that finite field operations are used for elliptic curve points. '960 Pat., 1:43-50 ("To carry out calculations involving points on the elliptic curve, calculations are done in the underlying finite field …."), 7:46-48 ("The data passed between the engines … comprises finite field elements, since an elliptic curve point consists of two finite field elements."). Defendant's redundant and unduly narrowing construction should be rejected. *See LifeNet Health v. LifeCell Corp.*, 837 F.3d 1316, 1327 (Fed. Cir. 2016) (rejecting a construction because it was redundant in view of the surrounding claim language and unduly narrowing in light of the specification).

2 & 3. "reduced result" / "unreduced result"
('960 patent - claims 3, 6; '062 patent - claims 1-4, 6, 7)

Claim Term	Defendant's Constructions	Plaintiffs' Constructions
reduced result	No construction needed. Plain and ordinary meaning.	"result of performing the claimed modular reduction"
unreduced result	"result without any reduction to a specific finite field or wordsize reduction"	"result without performing the claimed modular reduction"

a) "reduced result"

The parties agree a "reduced result" is what results from performing the claimed modular reduction. Dkt. 53 at 15-16; Dkt. 59 at10 ("the claim language plainly states what is performed to obtain a reduced result"). Plaintiffs' construction tracks this plain meaning.

The claims' description of what a "reduced result" is also informs what its opposite—an "unreduced result"—is. Dkt. 53 at 15-17. As such, articulating the plain and ordinary meaning of

"reduced result" enables a consistent construction of "unreduced result." Plaintiffs' construction should therefore be adopted for clarity and consistency.

b) "unreduced result"

Like "reduced result," the claims also spell out what an "unreduced result" is. In claim 3 of the '960 Patent, an unreduced result is what exists after "completing said non-reducing wordsized operation for each word of said representations" and *before* "performing a specific modular reduction." 960 Pat., 17:37-41. Claim 1 of the '062 Patent is similar: an unreduced result exists after "performing the finite field operation" and *before* "performing a modular reduction." '062 Pat., 16:29-35. To keep parity with "reduced result," "unreduced result" should be construed as its antonym: "result *without* performing the claimed modular reduction." Dkt. 53 at 17-18. This flows from the fact that the claims recite what a "reduced result" is, and both the claims and the specification indicate that an "unreduced result" is the opposite of that: a result on which the steps to obtain the reduced result have not been performed.

Defendant argues for further limitations that forbid "***any*** reduction to a specific finite field or wordsize reduction" on the basis that "the claims are silent as to what types of reduction are not performed to obtain an unreduced result." Dkt. 59 at 9-10 (emphasis added). But, as the claims themselves recite, it is not "any" reduction that produces a "reduced result"—only the claimed modular reduction. Because an "unreduced result" is the opposite of a "reduced result," and because the claims recite how a "reduced result" is obtained, the claims make clear that an "unreduced result" is a result on which the steps to produce the claimed "reduced result" have not been performed.

Defendant's argument that obtaining an "unreduced result" must not involve performing either of the "two types of reduction" purportedly described in the specification assumes the claims are silent as to the type of reduction not performed to obtain an unreduced result. Dkt. 53 at 18.

That is plainly not the case – each claim recites that an unreduced result is what exists without performing the ***claimed*** modular reduction.

Defendant's defense of its proposed construction is also inconsistent with the proposal itself. Defendant argues that the patents teach a first type of reduction that is "***reduction*** … ***specific to*** a certain finite field" (citing '960 Pat., 8:51-54), but its construction recites something different: "***reduction to*** a specific finite field." *See* Dkt. 59 at 8-10 (emphasis added). The meaning of Defendant's construction is unclear and irreconcilable with the specification. Dkt. 53 at 18. Defendant's inclusion of "wordsize reduction" is also unnecessary, as the claims indicate that the "unreduced result" is one on which the claimed "modular reduction" is not performed. *See supra*.

C. The '827 and '370 Patents

1. "the electronic message omits a public key of a signer"
('370 patent – claim 1)

Defendant's Construction	Plaintiffs' Construction
"the electronic message does not include any representation of the public key of the signer"	Plain and ordinary meaning

This term needs no construction. Claim 1 plainly states what's omitted from the message: "a public key of a signer." '370 Pat., 17:31-64. The claim does not require, and the specification does not discuss, omitting anything other than the public key itself. Dkt. 53 at 21. In particular, the specification teaches that omitting the public key (which comprises a point "Q") does not prohibit a different "version" of it from being sent "instead." '370 Pat., 16:22-27; Dkt. 53 at 21.

Defendant's construction, which requires the omission of "*any representation*" of the public key, broadens the scope of the limitation beyond its plain limit—Defendant wants the claim to require omitting not just the signer's public key, but also *any representation* of that key. In particular, Defendant is keen on broadening the term to require omission of "a compressed version" of public key Q. Dkt. 59 at 10. But there is no evidence in the specification to support

this, and Defendant identify none.[4]

Defendant's primary argument in favor of its construction is that "[i]nterpreting the claim to allow (rather than omit) sending such a representation of the public key Q would render the claimed recovery equation pointless." Dkt. 59 at 10-11. Defendant's argument boils down to its supposition that if representations of public keys are allowed, then there would be no need to use the recovery equation to determine the key. This logical leap, however, is not supported by the claim language or the specification, and rests solely on Defendant's attorney argument. That is not enough.

In its opening brief, Defendant's position was that a "representation of the public key Q" encompasses things that "can be used to compute the public key Q." Dkt. 52 at 26. That construction is so broad that it requires omitting the signature used to compute the public key, even though claim 1 requires it *not* to be omitted. Dkt. 53 at 21-22. Defendant tries to wave away this critical defect in its construction by declaring "[t]he signature (r,s) is not a representation of the public key Q," despite agreeing it is used to compute Q. Dkt. 59 at 11. This is a clear indication that Defendant's proffered construction is vague and indeterminable.

Defendant now tries to repair its deficient construction by defining "representation of the public key" as "a form of the public key Q (e.g., a compressed version of Q) 'such that the public key Q could be obtained from the representation [without] need to recover the public key Q ***using the specific equation recited in the claim***.'" *Id*. at 10. But none of this is in Defendant's construction. Even if it were, the construction lacks intrinsic support for the reasons explained in

[4] It is clear from the specification that patentees knew how to articulate "compressed versions" of something – they discussed "replacing r by a *compressed version* of R" and "sending a *compressed value* of R instead of r." '370 patent, 12:15-18 (emphasis added). Had patentees intended the claims to omit more than just the signer's public key, *i.e.*, that the omission should also include a "compressed version" of the key, they could have said so. But they did not.

Plaintiffs' responsive brief. Dkt. 53 at 21.

Lastly, Defendant misreads the prosecution history. The applicant argued that a reference cited by the PTO did not teach or suggest "omitting any public keys of the signer" because it taught the use of a "short term public key R" that "must be included in the message." Dkt. 53-7 at 4448. Defendant's initial argument is moot, however, because R is not a "representation of the public key Q" under its narrowed interpretation of its construction.[5]

2. "verifying that the second elliptic curve point Q represents the public key of the signer" *('827 patent – claim 2)*

Defendant's Construction	Plaintiffs' Construction
"verifying that the second elliptic curve point Q represents the second elliptic curve point Q"	Plain and ordinary meaning

This term requires no construction. Claim 2 requires "verifying that" something ("the second elliptic curve point Q") "represents" something else ("the public key of the signer"). This is consistent with claim 1, which requires both (i) "the public key of the signer comprises a second elliptic curve point Q" and, separately, (ii) "generating the public key of the signer comprises computing $Q=r^{-1}(sR-eG)$." *See* '827 patent, claim 1. Claim 2 then claims verifying that (i) represents (ii).

Defendant contends that its construction "aligns exactly with the claim language" because "both the 'second elliptic curve point' and 'the public key of the signer' are the value Q that is computed." Dkt. 59 at 12. This is improper because it reads out the claims' requirement of verifying that the computed Q represents the assigned value of the public key Q.

[5] Defendant also argues that "the then-pending claims did refer to 'the public key compris[ing] a second elliptic curve point,' (*i.e.*, Q)." Dkt. 59 at 11 n.1. Defendant is wrong. Defendant cites the amended claims at Dkt. 53-7 at 4595, while Plaintiffs were referring to the earlier state of the claims being addressed by the applicant at Dkt. 53-7 at 4448, shown in full at Dkt. 53-7 at 4440.

D. The '961 Patent

1. "random number generator" *('961 patent – claims 1-7)*

Defendant's Construction	Plaintiffs' Construction
"a system or algorithm that generates a random value"	"computer instructions capable of generating values according to a uniform random probability distribution"

The '961 patent describes a random number generator ("RNG") as generating values with "a uniform distribution throughout the defined interval." '961 Pat. 2:15-17, 2:29-32. Defendant acknowledges as much. Dkt. 59 at 13. Plaintiffs' construction is therefore consistent with the patent's meaning of the term.

Defendant's seemingly innocuous construction (an RNG "generates a random value") is betrayed by the varying arguments in its briefs that push for something far narrower. In its opening brief, Defendant argued that the claimed RNGs should be limited to "true" RNGs and not pseudorandom number generators ("PRNGs"). Dkt. 52 at 29-31. But on reply, Defendant abandoned that position and introduced a new one, arguing that "random" does not "encompass ***all*** 'pseudorandom' values," Dkt. 59 at 13-14 (emphasis added); *see also id.* at 12-13 (arguing RNGs must generate "unpredictable" values and that "deterministic" PRNGs do not generate unpredictable values). In short, Defendant now contends that RNGs must exclude PRNGs that do not generate unpredictable values.

Like its old argument, Defendant's new argument also misses the mark. PRNGs (also referred to as "deterministic" RNGs) can generate unpredictable values, just like true RNGs. Dkt. 53-2, ¶ 59; Dkt. 59-3 at 120:13-121:21. Thus, requiring RNGs to generate "unpredictable" values does not exclude PRGNs. Characterizing PRNGs as "deterministic" does not change this. According to Defendant's own expert, "deterministic" means that "using the same seed value(s) input will always result in the same output." Dkt. 52-2, ¶ 83 (citing Dkt. 52-19 at 629

("[D]eterministic here means that given the same initial seed, the generator will always produce the same output."). As such, ***all*** PRNGs—even those that generate unpredictable values—are "deterministic." Dkt. 52-2, ¶ 83 (describing "PRNGs" as "using deterministic algorithms"); Dkt. 53-2, ¶ 55 ("PRNGs are deterministic algorithms"); Dkt. 53-13 at 7 ("The first class [of 'real world' RNGs] consists of the *deterministic RNGs* (DRNGs, aka *pseudorandom number generators*)."). In fact, Defendant's expert agreed that "deterministic random number generator, or DRNG" is a "synonym" for, "another name for," and "just another way of saying" PRNG. Dkt. 53-5 at 93:24-94:2, 100:16-20, 101:16-20.

Thus, PRNGs, even though they are deterministic, are included in the scope of claimed RNGs. Defendant's expert testified as much: an RNG "for cryptography" can be "a ***deterministic*** random number generator," Dkt. 53-5 at 97:14-19, and a "cryptographically secure PRNG"—a PRNG used in cryptography or "CSPRNG"—is a deterministic RNG, *id*. at 94:21-95:6. Deterministic PRNGs can therefore produce unpredictable values. Dkt. 53-2, ¶ 59 ("[A]lthough the output of a CSPRNG is deterministic it is not predictable to an adversary with limited computation resources without knowledge of the underlying seed."). Plaintiffs' expert corroborated this understanding, explaining that "[PRNGs] used for cryptographic purposes are unpredictable," and "[t]here are different ways you can construct [PRNGs] that are unpredictable," for example, using "certain types of hash functions" and "a seed that has sufficient entropy," which may be generated by a true RNG or a PRNG that is cryptographically secure. Dkt. 59-3 at 120:13-122:12. A construction that is interpreted as excluding "deterministic" RNGs would wrongly exclude ***all*** PRNGs, including those used in cryptography that produce unpredictable values.[6]

[6] Defendant's criticism that Plaintiffs' construction "does not require unpredictable values" applies equally to Defendant's construction: neither party's construction expressly calls for "unpredictable" values (because it is unnecessary to do so, as explained above).

2. "seed" *('961 patent – claims 1-7)*

Defendant's Construction	Plaintiffs' Construction
"a random value that is used as the starting value for a cryptographic key generation function"	"a value obtained from a random number generator that is used to as the starting value for a cryptographic key generation function"

The dispute regarding "seed" flows from the dispute regarding "random number generator," as claim 1 requires "generating a seed value SV *from a random number generator*." '961 Pat., 5:36-37; Dkt. 52 at 33 (Defendant arguing that "the seed value is random because it is generated from a random number generator"). Defendant seeks an overly narrow construction that excludes "seed" values generated by "deterministic" RNGs (*i.e.*, PRNGs). Dkt. 59 at 15-16. As explained above, RNGs in the context of cryptography *include* deterministic RNGs that produce pseudorandom values. *See supra*; Dkt. 53 at 31-32. As Plaintiffs' expert explains, deterministic RNGs (*e.g.*, CSPRNGs) are used to generate "seed" values in cryptography. Dkt. 53-2, ¶ 59 (a "seed" can "either [be] generated by a True RNG or by using a CSPRNG").

Defendant's contention that a seed cannot be a "deterministic" or pseudorandom value lacks basis. Dkt. 59 at 15. Defendant mischaracterizes the prosecution history in arguing that the applicant disclaimed the use of PRNGs to generate a seed. *Id*. The applicant did not distinguish prior art based on the difference between true random and pseudorandom. Rather, the applicant argued that the asserted reference did not disclose determining whether ***the hash of the seed generated by the RNG*** is less than q, as required by the claims. ("Step (c) of claim 1 involves determining whether the output is less than q, where the output is a result of a hash on a seed number that is chosen at random. In Schneier, …[the] value k is not an output that is a result of a hash on a seed number chosen at random, it is a random number in itself."). Dkt. 52-13 at 1227. Defendant identifies no "clear and unmistakable" disclaimer of pseudorandom or "deterministic" values. *Omega Eng'g, Inc, v. Raytek Corp.*, 334 F.3d 1314, 1325-26 (Fed. Cir. 2003); *Grober v.*

Mako Prods., Inc., 686 F.3d 1335, 1342 (Fed. Cir. 2012) (prosecution history disclaimer requires "an unambiguous disavowal that clearly and unmistakably disclaims claim scope or meaning").

Defendant also argues that a "seed" value requires "sufficient entropy" and therefore cannot be "deterministic," but this too is incorrect. A seed with sufficient entropy *can* be generated by a deterministic RNG (*e.g.*, a CSPRNG). Dkt. 59-3 at 122:5-12 ("**Q.** What are various ways that you can get a seed with sufficient entropy? **A.** You can use a true number generator to get such a seed. ***You can use a pseudorandom number generator, cryptographically secure pseudorandom number generator that is operating properly to get such a seed as well.***"); *see also* Dkt. 53-2, ¶ 59. Defendant does not dispute this.

3. "The method of claim 1 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key."
('961 patent – claim 7)

Defendant's Construction	Plaintiffs' Construction
Indefinite	Not indefinite.

Claim 7 is not indefinite. The relationship between claims 1 and 7 is reasonably certain from the claims' plain language and the context of the specification: claim 7 describes a particular way of repeating the method of claim 1. Claim 1 recites (in relevant part):

> **1.** A method of generating a key k for use in a cryptographic function performed over a group of order q, said method including the steps of:
>
> [a] generating a seed value SV from a random number generator;
>
> [b] performing a hash function H( ) on said seed value SV to provide an output H(SV);
>
> [c] determining whether said output H(SV) is less than said order q …;
>
> [d] accepting said output H(SV) for use as said key k if the value of said output H(SV) is less than said order q;
>
> [e] rejecting said output H(SV) as said key if said value is not less than said order q;
>
> [f] if said output H(SV) is rejected, repeating said method; and
>
> [g] …

Per step 1[f], "if said output H(SV) is rejected," claim 1 requires "repeating said method." Claim 7 depends from claim 1 and is practiced only when the output of claim 1 is rejected. '961 Pat., 5:65-66 ("7. The method of claim 1 wherein if said output is rejected…."). Claim 7 then recites a particular way of repeating steps [a]-[c] of claim 1:

> [7a] "said output is incremented by a deterministic function"
>
> [7b] "a hash function is performed on said incremented output to produce a new output," and
>
> [7c] "a determination being made as to whether said new output is acceptable as a key."

'961 Pat., 5:65-6:3. In particular, [1a] requires "generating a seed value SV from a random number generator," which is not limited to any particular type of RNG. When step [1a] is repeated, claim [7a] requires a certain kind of RNG, *i.e.*, a "deterministic function." The incremented output of [7a] is the "SV" of [1a] which is hashed at step [7b] (*i.e.,* the repeated step [1b]). And step [7c] is the repeated step [1c] that compares the output of the hashing step to "q."

To conjure support for its indefiniteness theory, Defendant mischaracterizes Plaintiffs' position about the relationship between claims 1 and 7. Plaintiffs never contended that "claim 1 does not require repeating steps (a)-(c)." *Contra* Dkt. 59 at 16. Rather, Plaintiffs explained that claim 7 describes how those steps of claim 1 are repeated. Dkt. 53 at 33-34.

The specification supports Plaintiffs' position. A POSITA would have understood that Figure 3, which teaches an additional step of incrementing the rejected output by a deterministic function (a way to "generate a seed value" per claim 1) before hashing it (to "perform[] a hash function H( ) on said seed value" per claim 1) after a rejection, informs the method of claim 7. Dkt. 53 at 33-34; Dkt. 59-3 at 125:25-127:22.

Plaintiffs' position is also corroborated by its expert, Dr. Martin, who explained that in element 7[a], "output is incremented by a deterministic function … is going to generate your new seed value" and corresponds to step 1[a] because "[y]ou're applying a deterministic function,"

which is "a random number generation function," and "[t]hat's going to create a new SV." Dkt. 59-3 at 125:25-126:10. In other words, when claim 1 is repeated according to claim 7, "[t]he output is incremented by a deterministic function is step A. That is your generation of a seed value from a random number generator. Your deterministic function applied to that output is your random number generator. It's describing how your random number generator works." *Id*. at 127:1-20. In element 7[b], "[a] hash function is performed on said incremented output to produce a new output. That's just re-describing H(SV)" of claim 1 (*see* step 1[a], *supra*). *Id*. at 126:11-14. In other words, "your hash [of claim 7] is the next step. That's step B [of claim 1]." *Id*. at 127:21-22. In element 7[c], "a determination being made as to whether said new output is acceptable as a key, that's [the] determination step. So it's just describing a modification to the method of Claim 1." *Id*. at 126:15-25. Accordingly, claim 7 describes how steps [a]-[c] of claim 1 are performed when claim 1 is repeated; it is not indefinite.

III. CONCLUSION

For the foregoing reasons, the Court should adopt Plaintiffs' constructions, which are supported by the intrinsic record and in accord with governing legal principles, and reject Defendant's constructions, which are not.

Dated: February 11, 2026

Respectfully Submitted,

/s/ Philip J. Eklem
Philip J. Eklem
REICHMAN JORGENSEN LEHMAN & FELDBERG LLP
1909 K Street NW, Suite 800
Washington DC, 20006
Tel: (202) 894-7310
peklem@reichmanjorgensen.com

Khue V. Hoang
REICHMAN JORGENSEN LEHMAN & FELDBERG LLP
400 Madison Avenue, Suite 14D
New York, NY 10017
Tel: (212) 381-1965
khoang@reichmanjorgensen.com

Matthew G. Berkowitz
Michael M. Polka
REICHMAN JORGENSEN LEHMAN & FELDBERG LLP
100 Marine Parkway, Suite 300
Redwood Shores, CA 94065
Tel: (650) 623-1401
mberkowitz@reichmanjorgensen.com
mpolka@reichmanjorgensen.com

Of Counsel:

Mark D. Siegmund, TX Bar No. 24117055
Cherry Johnson Siegmund James, PC
7901 Fish Pond Rd., 2nd Floor
Waco, TX 76710
Telephone: (254) 732-2242
Facsimile: (866) 627-3509
Email: msiegmund@cjsjlaw.com

Attorneys for Plaintiffs
Malikie Innovations, Ltd. and
Key Patent Innovations, Ltd.

CERTIFICATE OF SERVICE

I hereby certify that all counsel of record are being served with a copy of the foregoing document via the Court's CM/ECF system on February 11, 2026.

/s/ Mark D. Siegmund
Mark D. Siegmund